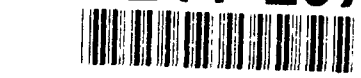




# MAPPING OF THE EMBEDDED REAL-TIME TRUSTED COMPUTER SYSTEMS (ERT-TCSs) REQUIREMENTS INTO THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

**Initial Mapping**



**August 24, 1990**



# REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 24 August 1990 | Final (Initial Mapping) |

**4. TITLE AND SUBTITLE**
Mapping of the Embedded Real-Time Trusted Computer Systems (ERT-TCSs) Requirements into the Trusted Computer System Evaluation Criteria

**5. FUNDING NUMBERS**
Contract

**6. AUTHOR(S)**
IIT Research Institute

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
IIT Research Institute
4600 Forbes Boulevard
Lanham, MD 20706

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
National Computer Security Center (NCSC)
9800 Savage Road
Fort Meade, MD 20755

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**
This report presumes familiarity with the final report, Requirements for Developing Embedded Real-Time Trusted Computer Systems (ERT-TCSs).

**12a. DISTRIBUTION/AVAILABILITY STATEMENT**
~~Government agencies~~
~~Government contractors~~
This document has been approved for public release and sale; its distribution is unlimited.

**12b. DISTRIBUTION CODE**
DOD
DOE
NASA

**13. ABSTRACT** (Maximum 200 words)
This report provides a mapping of the requirements in the final report, Requirements for Developing Embedded Real-Time Trusted Computer Systems (ERT-TCSs) to the classes in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC DOD 5200.28-STD, alias the "Orange Book"). Because the TCSEC was intended for traditional automated data processing equipment, it is insufficient for embedded real-time trusted computer systems. Therefore the TCSEC had to be adapted for ERT-TCSs. NCSC does not officially sanction this report, which was only a research effort.

| 14. SUBJECT TERMS | | 15. NUMBER OF PAGES |
|---|---|---|
| Embedded | ) Trusted Computer System Evaluation | 204 |
| Real-Time | ) Criteria | 16. PRICE CODE |
| Trusted Computer Systems | ) TCSEC//Orange Book | |
| | ) Computer Security | |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| | | | |

# MAPPING OF THE

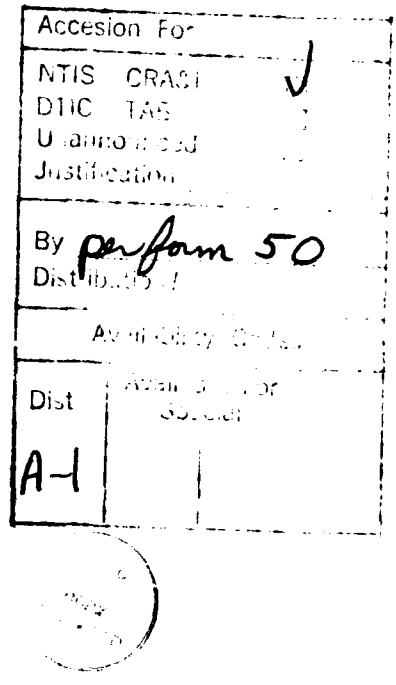
# EMBEDDED REAL-TIME TRUSTED COMPUTER SYSTEMS (ERT-TCSs)

# REQUIREMENTS INTO THE

# TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

**Prepared for:**

**National Computer Security Center**
**9800 Savage Road**
**Fort Meade, MD 20755**




**Prepared by:**

**IIT Research Institute**
**4600 Forbes Boulevard**
**Lanham, MD 20706**

**Initial Mapping**

**August 24, 1990**

## TABLE OF CONTENTS

## FIGURES

# 1.0 INTRODUCTION

## 1.1 BACKGROUND

In recent directives, the Department of Defense (DoD) has distinguished embedded computer systems applications from automated data processing (ADP) computer applications; however, the DoD has not issued a security manual that is specific to embedded real-time trusted computer systems (ERT-TCSs)[1]. The direction has been to use the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC DOD 5200.28-STD, alias the "Orange Book") as the guidebook for security. The TCSEC, however, does not meet the distinct security requirements of an ERT-TCS, particularly for the operational phase of the ERT-TCS's life cycle.

The TCSEC was written for ADP systems that are different from ERT-TCSs in a number of ways. For instance, the mobility of an ERT-TCS raises maintenance security concerns that would not affect typical ADPs. Mobility hinders the accessibility of the ERT-TCS, particularly during its operation. Some standard security measures for ADP systems are difficult, if not impractical, to apply to a mobile ERT-TCS. Also, communications between external devices and an ERT-TCS are potentially more vulnerable than comparable ADP communications. This is because the ERT-TCS communications are typically performed in facilities in which security is more difficult to ensure than it is to ensure those communications in the fixed confines of a typical ADP system. Some suspect communications are those between an ERT-TCS and external resources in the developmental or maintenance environments and communications between the ERT-TCS and other subsystems embedded within a system, e.g., an avionics system. Finally, the TCSEC, which is written for standard ADP systems, does not address the unique constraints imposed by embedded real-time systems. Even before security considerations are applied to embedded real-time systems, these systems typically have their own time and space performance demands that exceed those of typical ADP Trusted Computing Bases (TCBs).

An interpretation of the TCSEC for ERT-TCSs is necessary to ensure that unclassified, classified, or otherwise sensitive information related to or used by an ERT-TCS during development, operation, and maintenance is properly developed, stored, communicated, handled, and secured. The implementation of the ERT-TCS must include all necessary security measures required to protect the level of sensitive

---

[1] An ERT-TCS is an embedded real-time trusted computer system that has been certified so that it may contain or use unclassified, classified, or otherwise sensitive data.

information and criticality of the ERT-TCS's functions. That is, the viability of the system within which the ERT-TCS is embedded must not be excessively degraded by the operation of the ERT-TCS.

## 1.2 PURPOSE

The intent of this document is to map the requirements in the final report, Requirements for Developing Embedded Real-Time Trusted Computer Systems (ERT-TCSs), to the TCSEC classes. In particularly, the mapping is to the classes A1, B3, and B2. This mapping will hopefully help in developing an interpretation of the TCSEC for ERT-TCSs. As stated in this earlier document, an embedded real-time system was chosen as a model, in particular, the Joint Integrated Avionics Working Group's (JIAWG) avionics architecture, which is to be used in the U. S. Air Force's Advanced Tactical Fighter (ATF). The initial steps in developing an interpretation of the TCSEC for an ERT-TCS are as follows:

1. Identify the security requirements for a specific embedded real-time system that will be considered representative of similar embedded real-time systems;

2. Promote the security of embedded real-time systems throughout their life cycle, i.e., development, operation, and maintenance;

3. Identify security issues for the ATF and similar embedded real-time systems that are not addressed in the TCSEC.

The immediate intent of these requirements is to address the integrity, confidentiality, and assurance of the service of an ERT-TCS's classified or sensitive documentation, software, firmware, hardware, and data throughout its life cycle. This study was done at the research level; additional work will be required to translate these requirements into a given operational situation. That is, the requirements must be translated into various operational contexts on a case by case basis. An ERT-TCS's subsystems (i.e., embedded real-time trusted computing bases [ERT-TCBs]) must ensure the confidentiality of all classified and unclassified sensitive information. Finally, all authorized users or subjects of the ERT-TCS must be assured of the ERT-TCS's service. "Through fault tolerance, redundancy, and other measures the component systems will maintain capabilities so that component systems resources will be continually available for use. Each of these areas must be addressed in all life cycle phases of development and acquisition to ensure the component systems can be certified, that they meet requirements in each environment, and together . . . can be accredited for secure operations." [ATF 1989, p.5]

The application of the Least Privilege Principle and the handling of "unclassified information or data" are two important security concepts required for the proper use of these requirements. The Least Privilege

Principle basically states that a subject should only have access to the objects required to successfully complete the subject's tasks. The access of information must be limited by the "need-to-know" principle, which states that access to sensitive data is allowed only to subjects who need to know that data required to perform their jobs. Also, subjects without the need-to-know certain information must not be allowed to modify the information. This helps to assure the integrity of the information. The preservation of integrity and assurance of service requirements are the same for unclassified and classified data.

These requirements and their mapping to the TCSEC may be used as guidelines to establish security policies for developing, operating, and maintaining ERT-TCSs. The primary objective of such security policies is to provide secure ERT-TCS environments that balance operational needs and available resources. To facilitate the use of this document, requirements that are applicable in multiple contexts are listed in each of the appropriate places. This approach ensures that no assumptions are made relative to implied requirements, and it will also enable the user to use this document as a reference.

## 1.3 SCOPE AND DEFINITIONS

### 1.3.1 Scope

The requirements identified in this document address security issues relevant to an ERT-TCS's three life cycle environments: developmental, operational, and maintenance. The JIAWG avionics architecture of the USAF ATF is used in this document as the model embedded real-time system for applying these requirements. Therefore, the requirements may or may not apply to other embedded real-time computer systems. Two mappings were made to facilitate relating the requirements and the TCSEC. The primary mapping of the requirements to the TCSEC are in Section 2. Because the requirements could not be mapped well to the original TCSEC organization, the mapping required a reorganization of and the addition of new sections in the TCSEC to properly accommodate the requirements. The TCSEC section on assurance needed the most drastic changes because it failed to adequately reflect the system life cycle and the three environments that ERT-TCSs can reside. This mapping was organized first by the modified or new TCSEC sections. Under each section is the corresponding discussions for the three classes A1, B3, and B2. The requirements have only been mapped to the various general TCSEC sections rather than to the various classes for the sections, because this is considered to be an initial mapping of the requirements. To minimize redundant text, a second mapping was created in Section 3 that cross references the TCSEC sections within the context of the requirements' rationales' structure, which was taken from the aforementioned ERT-TCS's requirements document.

Each of an ERT-TCS's three life cycle environments must be considered to identify the relevant security issues. The functional representation of these three environments is illustrated in Figure 1-1. The transitional functional areas overlap the functional areas. Functions performed in each functional area are listed in Figure 1-1.

Figure 1-2 delineates the differences between the environments used in the ERT-TCS's life cycle and depicts where the functions listed in Figure 1-1 are addressed in this document. Each of the functions listed in the transitional functional areas have been taken out of the overlap area and placed in one of the three environments. Initially, only the developmental environment exists. After initial deployment, all of the environments exist at various times throughout the ERT-TCS's life cycle. The ERT-TCS exists as a separate entity in all three environments.

Figure 1-3 shows the various types of distributions of trusted software, firmware, hardware, or data between the three environments (developmental, operational, and maintenance).

Figure 1-1. Functional Representation of the Embedded Real-Time Trusted Computer System Environments.

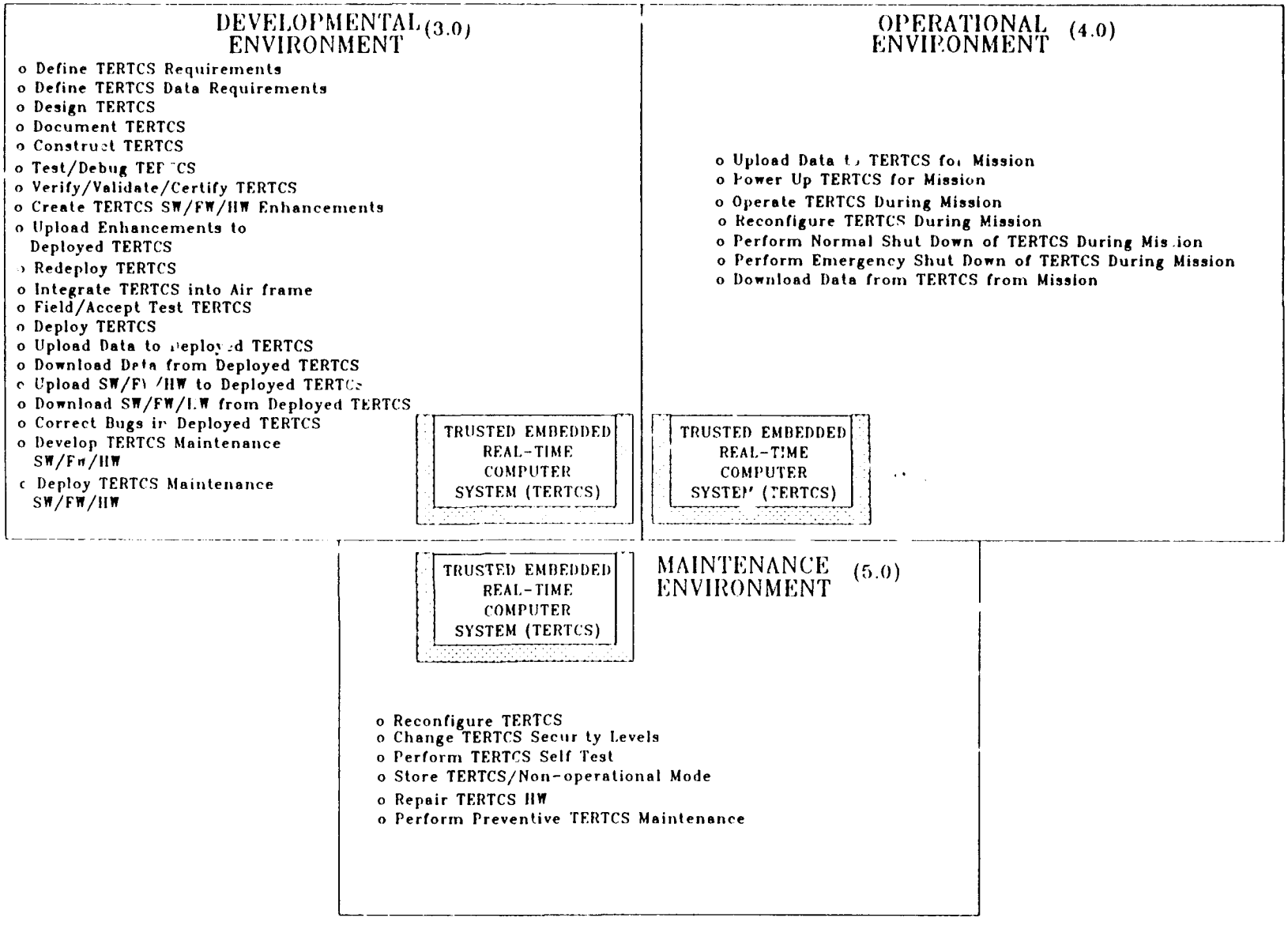



Figure 1-2. Document Organization (Physical Representation).

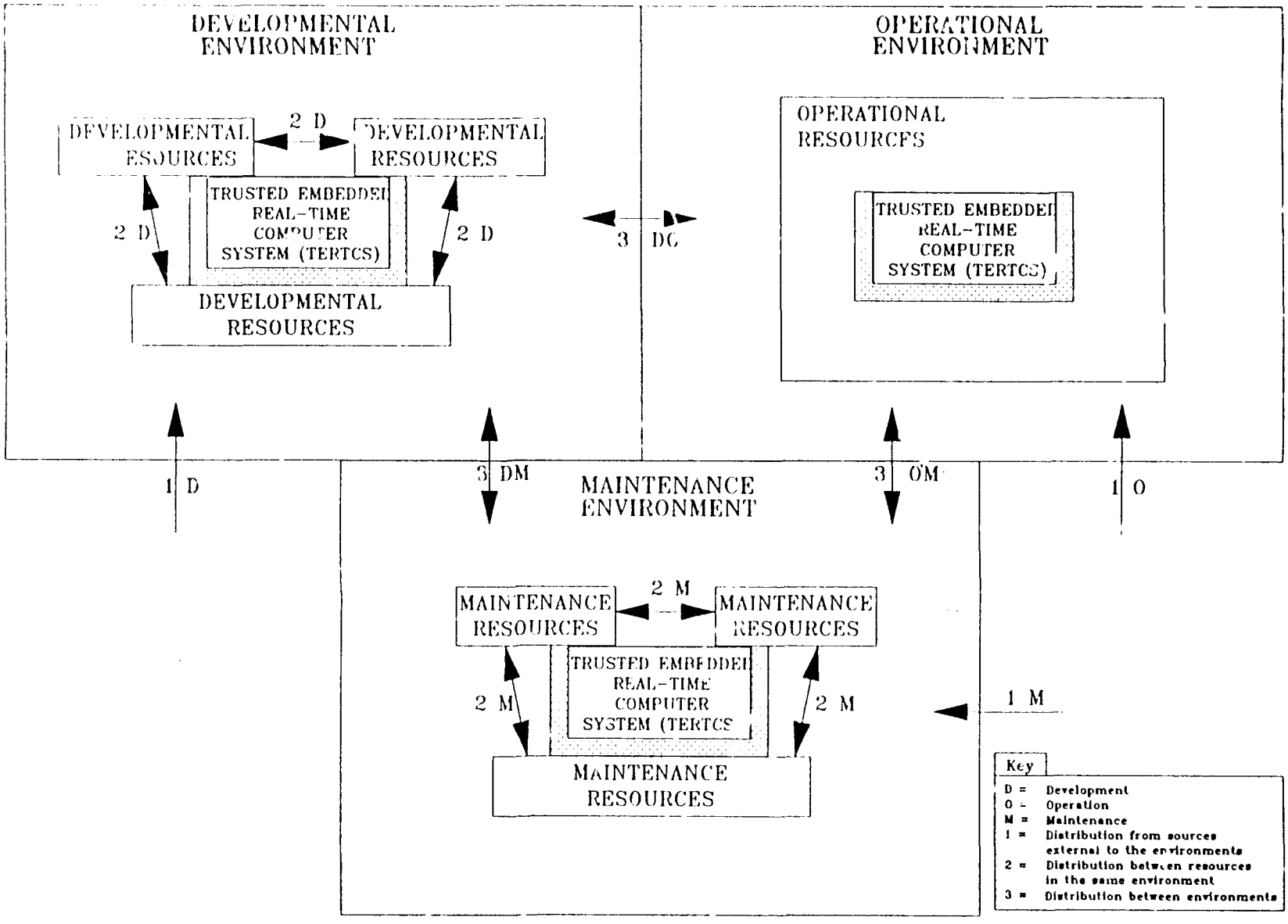



Figure 1-3. Distributions Between the Three Environments.

### 1.3.2 Definitions

An **environment** is "the aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system" [NCSC-TG-004 Version-1]. The three environments associated with the life cycle of the ERT-TCS are identified by the activities that are performed in those environments (i.e., a **developmental environment** is an environment in which developmental activities are performed, an **operational environment** is an environment in which operational activities are performed, a **maintenance environment** is an environment in which maintenance activities are performed). An environment contains all the resources for its prescribed set of activities. A partial list of activities for each environment is provided in the following definitions and is shown in Figure 1-1.

A **developmental activity** is associated with the creation and enhancement of the ERT-TCS and the ERT-TCS maintenance systems. Developmental activities include, but are not limited to, defining the requirements and designing, documenting, constructing, testing, debugging, verifying, validating, integrating, certifying, and deploying either the ERT-TCS itself or ERT-TCS maintenance systems.

An **operational activity** is associated with the operation of the ERT-TCS for a mission. Operational activities include, but are not limited to, performing the following activities during a mission: powering up for a mission, operating for a mission, reconfiguring the ERT-TCS, changing security levels, performing normal or emergency shutdown during or after a mission, and uploading or downloading data for a mission.

A **maintenance activity** is associated with the performance of the maintenance systems and all other non-mission operations. Maintenance activities include, but are not limited to, performing the following activities between missions: reconfiguring the ERT-TCS, changing security levels, performing self test, storage, repairs to hardware, and performing preventive maintenance.

A **resource** is an entity that is used to support a particular set of activities (i.e., developmental, operational, or maintenance). Resources include, but are not limited to, facilities, computer hardware, computer software or firmware, commercial off-the-shelf documentation, personnel, and furniture. **External resources** are resources that have entered the environment from the external world. External resources have not been modified in the environment. **Internal resources** are resources that have been created or modified within an environment. If an external resource is modified, then it is treated the same as a modified internal resource. Code that originates from a repository that is external to the environment (i.e., an external repository) is certified in the same manner as any other external resource. If that code is then incorporated into the ERT-TCS or the ERT-TCS maintenance systems, then it is considered to be a product. A

repository that is created and maintained internally to an environment is considered to be an internal repository. Any code that originates from an internal repository is treated the same as an internal resource or product.

In this document **product** is defined to be any part of the ERT-TCS or any part of the ERT-TCS maintenance systems. An ERT-TCS includes all ERT-TCBs within an embedded system, all other security functions, and all functions that access any unclassified, classified, or otherwise sensitive data handled by the embedded system. A resource may become a product if the resource becomes part of the ERT-TCS or the ERT-TCS maintenance systems.

A **facility** is a structure, portion of a structure, or physical area that is used to perform a particular set of activities. A facility is a resource. A facility may contain non-facility resources. The three types of facilities used in the life cycle of the ERT-TCS are identified by the activities that are performed in those facilities (e.g., a **developmental facility** is where developmental activities are performed). If the type of activity in the maintenance facility changes from maintenance to development, then the facility becomes a development facility and must be treated the same as any other development facility.

**Data** is information with a specific physical representation. Data is not considered to be a resource or a product. **External data** is data that has entered the environment from the external world. **Internal data** is data that has been created or modified within an environment. If external data is modified, then it is considered to be internal data and is treated the same as modified internal data.

An **object** is a passive entity that contains or receives information. Data is always an object. A resource or product is an object when it is being stored electronically. The protection of an object ultimately affects the protection of the ERT-TCS and the data controlled by the ERT-TCS.

A **subject** is an active entity that causes information to flow among objects or changes the system state. A resource or product is a subject while it is being executed. Data is never a subject.

An **environment** contains facilities, other resources, and data used to perform a prescribed set of activities on products.

A **security policy** is the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information [DOD 5200.28-STD]. It specifies if, when, how, and by whom, and the extent to which the system security requirements are to be addressed. The issues addressed by the

security policy of a particular facility is dependent on the type of environment (i.e., developmental, operational, or maintenance) and specific security needs of the facility. A single comprehensive security policy may apply to an ERT-TCS's associated resources and products throughout its life cycle, though it may be partitioned according to environment or facility.

In this document the security issues relevant to the ERT-TCS have been divided into three mandates: preservation of integrity, prevention of compromise, and assurance of service. **Regulation of access** is controlling the interaction and flow of unclassified, classified, or otherwise sensitive information between subjects (i.e., persons, processes, or devices) and objects (i.e., software, firmware, hardware, or data). This includes direct access and access derived indirectly by intercepting communications, emanations, etc. Regulation of access includes the control of the type of access (e.g., read, execute, write, append, modify, delete, or create) to an object. Regulation of access is an activity that is related to all three of these security mandates. **Integrity** is the assurance that unclassified, classified, or otherwise sensitive objects are in sound, unimpaired, and perfect condition. That is, no erroneous or unauthorized changes to mission or control data or execution of mission or control logic occur. If any violations are detected, the ERT-TCS will be brought back to a secure state in a specified time. The primary threats considered are accidental and malicious. Thus, the prevention of the accidental or malicious alteration or destruction of software, firmware, hardware, or data is required to assure integrity. **Compromise** is a violation of the security policy that may result in unauthorized disclosure of sensitive information. **Confidentiality** is the concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. **Assurance of service** is the confidence that sufficient services or resources will be available to perform the mission as intended. Assurance of service implies protection against the denial of service threat.

A **trusted process** handles classified or otherwise sensitive data; it may also monitor the integrity and security of data or resources.

## 1.4 ORGANIZATION

This document is organized into four sections. Section 1 is the introduction which provides preliminary and background information about the document's content and how to use it. Sections 2 and 3 are the core of the document. Section 2 contains the primary mapping of the requirements to the TCSEC. Some TCSEC sections were reorganized and new sections were added to properly accommodate the requirements. Under each section is the corresponding discussions for the three classes A1, B3, and B2. The requirements have only been mapped to the various general TCSEC sections rather than to the various classes for the

sections, because this is considered to be an initial mapping of the requirements. Section 3 provides a mapping for cross referencing the TCSEC sections within the context of the requirements' rationales' structure found in Appendix A of the final report, Requirements for Developing Embedded Real-Time Trusted Computer Systems (ERT-TCSs). In both mappings the requirements are further organized by the three general environments of development, operation, and maintenance. These are further divided into three security mandates: "preserve integrity", "prevent compromise", and "assure service." Each requirement is followed by a reference to the rationale in Appendix A in the aforementioned ERT-TCS's requirements document. The following is the meaning of the letters within the paragraph numbers in Sections 2 and 3:

A - supports all security mandates
I - supports the mandate to preserve integrity
C - supports the mandate to prevent compromise
S - supports the mandate to assure service.

Two appendices are included in this document. Appendix A contains the list of acronyms used in this document. Appendix B contains the bibliography. For a glossary of terms used in this document as well as additional related terms refer to Appendix B in the aforementioned ERT-TCS's requirements document.

THIS PAGE IS INTENTIONALLY BLANK.

# SECTION 2.0

# MAPPING OF THE
# EMBEDDED REAL-TIME TRUSTED COMPUTER SYSTEM REQUIREMENTS
# INTO THE
# TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

THIS PAGE IS INTENTIONALLY BLANK.

## 2.1 PROPOSED REORGANIZATION OF THE TCSEC (Classes A1, B3, and B2)

**1 Security Policy**

1.1 Discretionary Access Control

1.2 Object Reuse

1.3 Labels

1.3.1 Label Integrity

1.3.2 Exportation and Importation of Labeled Information

1.3.2.1 Exportation to **and Importation from** Multilevel Devices

1.3.2.2 Exportation to **and Importation from** Single-Level Devices

1.3.2.3 Labeling Human-Readable Output

1.3.3 Subject Sensitivity Labels

1.3.4 Device Labels

1.4 Mandatory Access Control

**1.5 Assurance of Authorized Access**

**2 Accountability**

2.1 Identification and Authentication

2.1.1 Trusted Path

2.2 Audit

**3 Assurance**

**3.1 Facility Management**

**3.1.1 Facility Accreditation**

**3.1.2 Facility Access Control**

**3.1.3** Trusted Distribution

**3.1.4 Certification**

**3.2 System Engineering**

**3.2.1** Design Specification and Verification

**3.2.2** Configuration Management

**3.2.3** System Architecture

**3.2.4** System Integrity

**3.2.5** Trusted Recovery

**3.2.6** Security Testing

**3.3 Communication Management**

**3.3.1 Communications Control**

**3.3.2 Manual Transfer of Data**

3.3.3 Covert Channel Analysis

**4 Documentation**

4.1 Security Features User's Guide

4.2 Trusted Facility Manual

4.3 Test Documentation

4.4 Design Documentation

**4.5 Documentation Management**

## 2.2 MAPPING OF THE ERT-TCS REQUIREMENTS INTO THE TCSEC

### CLASS (A1): VERIFIED DESIGN

Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. Independent of the particular specification language or verification system used, there are five important criteria for class (A1) design verification:

* A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.

* An FTLS must be produced that includes abstract definitions of the functions the TCB performs and of the hardware and/or firmware mechanisms that are used to support separate execution domains.

* The FTLS of the TCB must be shown to be consistent with the model by formal techniques where possible (i.e., where verification tools exist) and informal ones otherwise.

* The TCB implementation (i.e., in hardware, firmware, and software) must be informally shown to be consistent with the FTLS. The elements of the FTLS must be shown, using informal techniques, to correspond to the elements of the TCB. The FTLS must express the unified protection mechanism required to satisfy the security policy, and it is the elements of this protection mechanism that are mapped to the elements of the TCB.

* Formal analysis techniques must be used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels. The continued existence of identified covert channels in the system must be justified.

In keeping with the extensive design and development analysis of the TCB required of systems in class (A1),

more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

The following are minimal requirements for systems assigned a class (A1) rating:

## CLASS (B3): SECURITY DOMAINS

The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration. The following are minimal requirements for systems assigned a class (B3) rating:

## CLASS (B2): STRUCTURED PROTECTION

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non- protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration. The following are minimal requirements for systems assigned a class (B2) rating:

## 1 Security Policy

### 1.1 Discretionary Access Control

**CLASS (A1): VERIFIED DESIGN**

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

**CLASS (B3): SECURITY DOMAINS**

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism **(e.g., access control lists)** shall allow users to specify and control sharing of those **objects**, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of **specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.** Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

### CLASS (B2): STRUCTURED PROTECTION

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

## 1.2 Object Reuse

### CLASS (A1): VERIFIED DESIGN

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

### CLASS (B3): SECURITY DOMAINS

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subjects actions is to be available to any subject that obtains access to an object that has been released back to the system.

CLAS (B2): STRUCTURED PROTECTION

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

1.3 Labels

The extent of labeling is determined by the classification and sensitivity of resources, products, and data handled by the system versus the system's operating demands.

CLASS (A1): VERIFIED DESIGN

Sensitivity labels associated with each ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

CLASS (B3): SECURITY DOMAINS

Sensitivity labels associated with each ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

CLASS (B2): STRUCTURED PROTECTION

Sensitivity labels associated with each **ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB** shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB.

1.3.1 Label Integrity

CLASS (A1): VERIFIED DESIGN

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

CLASS (B3): SECURITY DOMAINS

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

CLASS (B2): STRUCTURED PROTECTION

Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

1.3.2 Exportation and Importation of Labeled Information

**CLASS (A1): VERIFIED DESIGN**

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

**CLASS (B3): SECURITY DOMAINS**

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

**CLASS (B2): STRUCTURED PROTECTION**

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the security level or levels associated with a communication channel or I/O device.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

3.4.C.4 The ERT-TCS will be developed so that all multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

4.4.C.4 All multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

5.4.C.4 The ERT-TCS will be maintained so that all multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

Assurance of Service

1.3.2.1 Exportation to and Importation from Multilevel Devices

**CLASS (A1): VERIFIED DESIGN**

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

**CLASS (B3): SECURITY DOMAINS**

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel

shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

CLASS (B2): STRUCTURED PROTECTION

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

1.3.2.2 Exportation to and Importation from Single-Level Devices

CLASS (A1): VERIFIED DESIGN

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

CLASS (B3): SECURITY DOMAINS

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

**CLASS (B2): STRUCTURED PROTECTION**

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices.

1.3.2.3 Labeling Human-Readable Output

These criteria apply only if human-readable output is produced.

**CLASS (A1): VERIFIED DESIGN**

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the overall sensitivity of the output or that properly[1] represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

---

[1] The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

## CLASS (B3): SECURITY DOMAINS

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the overall sensitivity of the output or that properly[1] represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

## CLASS (B2): STRUCTURED PROTECTION

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the overall sensitivity of the output or that properly[1] represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

---

[1] The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

### 1.3.3 Subject Sensitivity Labels

These criteria apply only if an interactive terminal is available for the query.

**CLASS (A1): VERIFIED DESIGN**

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

**CLASS (B3): SECURITY DOMAINS**

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

**CLASS (B2): STRUCTURED PROTECTION**

**The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.**

### 1.3.4 Device Labels

**CLASS (A1): VERIFIED DESIGN**

The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

CLASS (B3): SECURITY DOMAINS

The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

CLASS (B2): STRUCTURED PROTECTION

**The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.**

1.4 Mandatory Access Control

CLASS (A1): VERIFIED DESIGN

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included

in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

## CLASS (B3): SECURITY DOMAINS

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

## CLASS (B2): STRUCTURED PROTECTION

The TCB shall enforce a mandatory access control policy over all **resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB.** These subjects and objects shall be assigned sensitivity labels that are a

combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. (See the Mandatory Access Control guidelines.) The following requirements shall hold for all accesses between **all subjects external to the TCB and all objects directly or indirectly accessible by these subjects:** A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Identification and authentication data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

**Developmental Environment:**

All Security Mandates

3.3.A.7 Every developmental environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

4.3.A.2 Every operational environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.3.A.2 Every maintenance environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

1.5 Assurance of Authorized Access

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

4.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

4.1.S.3 During a mission, the most critical tasks will always have access to all that they need to function adequately.

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

5.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

## 2 Accountability

### 2.1 Identification and Authentication

**CLASS (A1): VERIFIED DESIGN**

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of

individual users. This data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

## CLASS (B3): SECURITY DOMAINS

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

## CLASS (B2): STRUCTURED PROTECTION

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity and to ensure that the security level and authorizations of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user. The TCB shall protect authentication data so that it cannot be

accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2.1.1 Trusted Path

CLASS (A1): VERIFIED DESIGN

The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other paths.

CLASS (B3): SECURITY DOMAINS

The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the TCB and all be logically isolated and unmistakably distinguishable from other paths.

CLASS (B2): STRUCTURED PROTECTION

The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.

## 2.2 Audit

Auditing will be performed to the extent that it does not unduly impinge on the functionality of the ERT-TCS and the system in which it is embedded.

### CLASS (A1): VERIFIED DESIGN

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.

### CLASS (B3): SECURITY DOMAINS

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for

audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. **The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded, and if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.**

## CLASS (B2): STRUCTURED PROTECTION

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system

administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. **The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels.**

**Developmental Environment:**

All Security Mandates

3.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

3.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

4.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

4.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

5.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

## 3 Assurance

### 3.1 Facility Management

**CLASS (A1): VERIFIED DESIGN**

The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

**CLASS (B3): SECURITY DOMAINS**

The TCB shall support separate operator and administrator functions. **The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.**

**CLASS (B2): STRUCTURED PROTECTION**

**The TCB shall support separate operator and administrator functions.**

#### 3.1.1 Facility Accreditation

**CLASS (A1): VERIFIED DESIGN**

## CLASS (B3): SECURITY DOMAINS

## CLASS (B2): STRUCTURED PROTECTION

**Developmental Environment:**

All Security Mandates

3.1.A.1 Every developmental facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

3.1.A.2 Every developmental facility need only be accredited to perform those activities (e.g., create, modify, enhance, test, or deploy) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

3.1.A.3 Every product will be developed in an accredited facility.

3.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment. For example, while a maintenance facility performs developmental activities (e.g., enhance ERT-TCS software) it will be considered a developmental facility and therefore be accredited in the same manner and to the same degree as any other developmental facility.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

4.1.A.1 Every operational facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

4.1.A.2 Every operational facility need only be accredited to perform those activities (e.g., power up, operate for a mission, upload or download data, power down from mission) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

4.1.A.3 Every product will be operated in an accredited facility.

4.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.1.A.1 Every maintenance facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

5.1.A.2 Every maintenance facility need only be accredited to perform those activities (e.g., repair hardware, perform preventative maintenance, reconfigure, change security levels, perform self test diagnostics, or storage) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

5.1.A.3 Every product will be maintained in an accredited facility.

5.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment. For example, while a maintenance facility performs developmental activities (e.g., enhance ERT-TCS software) it will be considered a developmental facility and therefore be accredited in the same manner and to the same degree as any other developmental facility.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.1.2 Facility Access Control

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

3.1.A.5 Every developmental facility will be secured with controlled access restrictions.

3.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

3.1.A.10 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the developmental facilities. This includes cryptographic

information.

3.1.A.11 The security level at which the ERT-TCS will be developed will be established and enforced on both the developmental personnel and the environment in which the ERT-TCS is developed.

3.2.A.6 Every developmental environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

3.2.A.8 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.3.A.10 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.3.A.11 The ERT-TCS will be developed so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

3.3.A.12 The ERT-TCS will be developed so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

3.3.A.13 The ERT-TCS will be developed so that it is capable of powering up and powering down in an unclassified mode. Although the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

3.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

Preservation of Integrity

Prevention of Compromise

3.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the developmental resources and facilities.

3.3.C.3 The ERT-TCS will be developed so that upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

3.3.C.4 Every product will be developed to process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

Assurance of Service

3.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

3.2.S.2 Every internal resource will be developed to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.3.S.3 Every product will be developed to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

3.6.S.1 Authorized development personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

**Operational Environment:**

All Security Mandates

4.1.A.5 Every operational facility will be secured with controlled access restrictions.

4.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

4.1.A.10 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the operational facilities. This includes cryptographic information.

4.1.A.11 The security level at which the ERT-TCS operates will be established and enforced on both the operational personnel and the environment in which the ERT-TCS operates.

4.2.A.2 Every operational environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

4.2.A.3 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

4.3.A.3 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

4.3.A.4 All products' hardware will be installed and protected at a level commensurate with its level of classification and sensitivity.

4.3.A.5 The ERT-TCS will be operated so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

4.3.A.6 The ERT-TCS will operate so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

4.3.A.7 The ERT-TCS will operate so that it is capable of powering up and powering down in an unclassified mode. Though the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

:

4.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

Preservation of Integrity

Prevention of Compromise

4.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the operational resources and facilities.

4.3.C.2 Upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

4.3.C.3 Every product will process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

Assurance of Service

4.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

4.2.S.2 Every internal resource will process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

4.3.S.2 Every product will process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

4.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

4.6.S.1 Authorized operational personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

**Maintenance Environment:**

All Security Mandates

5.1.A.5 Every maintenance facility will be secured with controlled access restrictions.

5.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

5.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, and otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the maintenance facility.

5.1.A.11 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the maintenance facilities. This includes cryptographic information.

5.1.A.12 The security level at which maintenance will be performed on the ERT-TCS will be established and enforced on both the maintenance personnel and the environment in which the maintenance is to be performed.

5.2.A.2 Every maintenance environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

5.2.A.3 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

5.3.A.3 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

5.3.A.4 The ERT-TCS will be maintained so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

5.3.A.5 The ERT-TCS will be maintained so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

5.3.A.6 The ERT-TCS will be maintained so that it is capable of powering up and powering down in an unclassified mode. Though the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

5.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

Preservation of Integrity

Prevention of Compromise

5.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the maintenance resources and facilities.

5.3.C.2 The ERT-TCS will be maintained so that upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

5.3.C.3 Every product will be maintained to process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

Assurance of Service

5.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

5.2.S.2 Every internal resource will be maintained to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

5.3.S.2 Every product will be maintained to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

5.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

5.6.S.1 Authorized maintenance personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

3.1.3 Trusted Distribution

These criteria do not apply to the operational environment.

CLASS (A1): VERIFIED DESIGN

**A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.**

CLASS (B3): SECURITY DOMAINS

The TCSEC does not discuss trusted distribution in the B3 class.

CLASS (B2): STRUCTURED PROTECTION

The TCSEC does not discuss trusted distribution in the B2 class.

**Developmental Environment:**

All Security Mandates

3.5.A.1 Every product, resource, and unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

Preservation of Integrity

3.5.I.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

Prevention of Compromise

3.5.C.1 The distribution of products, resources, and unclassified, classified, and otherwise sensitive data among resources will not result in their compromise.

3.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

Assurance of Service

3.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

3.5.S.2 No type of distribution will impair the performance of resources.

**Operational Environment:**

All Security Mandates

4.5.A.1 Every product, resource, or unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

Preservation of Integrity

4.5.I.1 The distribution of products, resources, and unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

Prevention of Compromise

4.5.C.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in their compromise.

4.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

Assurance of Service

4.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

4.5.S.2 No type of distribution will impair the performance of resources.

**Maintenance Environment:**

All Security Mandates

:

5.5.A.1 Every product, resource, or unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

Preservation of Integrity

5.5.I.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

Prevention of Compromise

5.5.C.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in their compromise.

5.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

Assurance of Service

5.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

5.5.S.2 No type of distribution will impair the performance of resources.

3.1.4 Certification

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

3.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the developmental environment.

3.2.A.2 Every internal resource will be signed off by the resource's creators, modifiers, and reviewers.

3.2.A.3 Every internal resource will be certified to comply with the security policy.

3.2.A.4 Every resource that implements part of the security policy will be certified to be necessary for enforcing the security policy.

3.2.A.5 Every modified or enhanced internal resource will be subject to the same certification process as the original resource.

3.3.A.1 Every product will be signed off by the product's creators, modifiers, and reviewers.

3.3.A.2 Every product will be certified to comply with the security policy.

3.3.A.3 Every product that implements part of the security policy will be certified to be necessary for enforcing the security policy.

3.3.A.5 Every product will be certified to process the highest classification of information to which it has direct or indirect access.

3.3.A.6 Every modified or enhanced product will be subject to the same certification process as the original product.

Preservation of Integrity

3.3.I.1 Every product will be certified to preserve the product's integrity before each time it is deployed.

Prevention of Compromise

3.3.C.1 Every product will be certified to prevent the product's compromise before each time it is deployed.

Assurance of Service

3.3.S.1 Every product will be certified to assure the product's service before each time it is deployed.

**Operational Environment:**

All Security Mandates

4.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the operational environment.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the maintenance environment.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

## 3.2 System Engineering

### 3.2.1 Design Specification and Verification

Those requirements that require formal verification apply only to division A. These requirements may be interpreted to apply to divisions below A if informal verification techniques are applied. These criteria do not apply to the operational environment.

**CLASS (A1): VERIFIED DESIGN**

A formal model of the security policy supported by the TCB shall be maintained over the life-cycle of the ADP system that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. **A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS and FTLS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface. The FTLS shall**

be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model **and a combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model. This verification evidence shall be consistent with that provided within the state-of-the-art of the particular National Computer Security Center-endorsed formal specification and verification system used. Manual or other mapping of the FTLS to the TCB source code shall be performed to provide evidence of correct implementation.**

CLASS (B3): SECURITY DOMAINS

A formal model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface. **A convincing argument shall be given that the DTLS is consistent with the model.**

CLASS (B2): STRUCTURED PROTECTION

**A formal** model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system that is proven consistent with its axioms. **A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface.**

**Developmental Environment:**

All Security Mandates

3.2.A.7 Every internal resource will be developed to satisfy the requirements for correctness, completeness, exactness, and performance integrity and will be subject to rigorous peer review for compliance with the requirements.

3.3.A.9 Every product will be developed to satisfy the requirements for correctness, completeness, exactness, and performance integrity and will be subject to rigorous peer review for compliance with the requirements.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

:

Prevention of Compromise

Assurance of Service

3.2.2 Configuration Management

These criteria do not apply to the operational environment.

**CLASS (A1): VERIFIED DESIGN**

During **the entire life-cycle, i.e., during the design, development,** and maintenance of the TCB, a configuration management system shall be in place **for all security-relevant hardware, firmware, and software** that maintains control of changes to **the formal model,** the descriptive **and formal** top-level **specifications,** other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools, **maintained under strict configuration control,** for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. **A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.**

CLASS (B3): SECURITY DOMAINS

During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

CLASS (B2): STRUCTURED PROTECTION

**During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.**

**Developmental Environment:**

All Security Mandates

3.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, or otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the developmental facility.

3.3.A.8 Thorough and stringent configuration management and configuration control of all product documents will be enforced to ensure consistency between the documentation and the implementation of the ERT-TCS.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

4.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, or otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the operational facility.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.1.A.10 Maintenance may be performed by uncleared personnel only when the ERT-TCS is in an unclassified mode.

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.2.3 System Architecture

**CLASS (A1): VERIFIED DESIGN**

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in

hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

## CLASS (B3): SECURITY DOMAINS

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. **The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.**

## CLASS (B2): STRUCTURED PROTECTION

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The

TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

3.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.I.5 The storage media of all resources will be protected from tampering.

3.3.I.3 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.3.I.5 Every product will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.3.I.6 Every transitional ERT-TCS function will be developed to prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

3.3.I.7 The storage media of all products will be protected from tampering.

3.3.I.8 The ERT-TCS will be developed to protect the storage media of all products' software and firmware from tampering.

3.3.I.9 Every product will be developed to process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

3.6.I.2 The ERT-TCS will be developed to protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

Prevention of Compromise

Assurance of Service

3.3.S.4 All ERT-TCS's modes of operation and ERT-TCS transitional functions will be developed to ensure adequate products' software and firmware and hardware to perform, at least, the most critical ERT-TCS functions.

3.3.S.5 All products will be able to satisfy their performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

3.3.S.7 Every product will be developed to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

3.4.S.6 The ERT-TCS will be developed so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

**Operational Environment:**

All Security Mandates

Preservation of Integrity

4.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

4.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

4.2.I.5 The storage media of all resources will be protected from tampering.

4.3.I.2 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

4.3.I.4 Every product will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

4.3.I.5 Every transitional ERT-TCS function will prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

4.3.I.6 The storage media of all products will be protected from tampering.

4.3.I.7 The ERT-TCS will operate to protect the storage media of all products' software and firmware from tampering.

4.3.I.8 Every product will process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

4.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

4.6.I.2 The ERT-TCS will protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

Prevention of Compromise

Assurance of Service

4.3.S.3 All ERT-TCS's modes of operation and ERT-TCS transitional functions will be operated to ensure adequate products' software and firmware and hardware to perform, at least, the most critical ERT-TCS functions.

4.3.S.4 All products will satisfy its performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

4.3.S.5 Every product will operate to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

4.4.S.6 The ERT-TCS will be operated so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

5.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

5.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

5.2.I.5 The storage media of all resources will be protected from tampering.

5.3.I.2 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

5.3.I.4 Every product will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

5.3.I.5 Every transitional ERT-TCS function will be maintained to prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

5.3.I.6 The storage media of all products will be protected from tampering.

5.3.I.7 The ERT-TCS will be maintained to protect the storage media of all products' software and firmware from tampering.

5.3.I.8 Every product will be maintained to process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

5.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

5.6.I.2 The ERT-TCS will be maintained to protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

Prevention of Compromise

Assurance of Service

5.3.S.3 All ERT-TCS's modes of operation and ERT-TCS transitional function[illegible]ill be maintained to ensure adequate products' software and firm[illegible]e and hardware to perform, at least, the most critical ERT-TCS functions.

5.3.S.4 All products will be able to satisfy its performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

5.3.S.5 Every product will be maintained to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

5.4.S.6 The ERT-TCS will be maintained so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

3.2.4 System Integrity

Self-testing will be performed during ERT-TCS operation.

**CLASS (A1): VERIFIED DESIGN**

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

**CLASS (B3): SECURITY DOMAINS**

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

**CLASS (B2): STRUCTURED PROTECTION**

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

**Developmental Environment:**

All Security Mandates

3.3.A.4 Products will be developed to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

Preservation of Integrity

3.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

3.2.I.3 Every resources' software and firmware will be developed to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.3.I.2 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

3.3.I.4 Every products' software and firmware will be developed to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

Prevention of Compromise

3.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.3.C.2 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on compromise will be minimized and be auditable.

Assurance of Service

3.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.3.S.2 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

**Operational Environment:**

All Security Mandates

4.3.A.1 Products will be able to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

Preservation of Integrity

4.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

4.2.I.3 Every resources' software and firmware will operate to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

4.3.I.1 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

4.3.I.3 Every products' software and firmware will operate to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

Prevention of Compromise

4.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

4.3.C.1 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

Assurance of Service

4.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

4.3.S.1 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

**Maintenance Environment:**

All Security Mandates

5.3.A.1 Products will be maintained to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

Preservation of Integrity

5.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

5.2.I.3 Every resources' software and firmware will be maintained to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

5.3.I.1 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

5.3.I.3 Every products' software and firmware will be maintained to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

Prevention of Compromise

5.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

5.3.C.1 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

Assurance of Service

5.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

5.3.S.1 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.5 Trusted Recovery

**CLASS (A1): VERIFIED DESIGN**

Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

## CLASS (B3): SECURITY DOMAINS

**Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.**

## CLASS (B2): STRUCTURED PROTECTION

The TCSEC does not discuss trusted distribution in the B2 class.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

3.2.I.6 Every internal resource's software and firmware will be developed to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.3.I.11 Every product's software and firmware will be developed to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

4.2.I.6 Every internal resource's software and firmware will operate to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

4.3.I.9 Every product's software and firmware will operate with adequate recovery procedures to handle malicious or erroneous code when it is discovered.

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

5.2.I.6 Every internal resource's software and firmware will be maintained to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

5.3.I.9 Every product's software and firmware will be maintained to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

Prevention of Compromise

:

Assurance of Service

3.2.6 Security Testing

During a ERT-TCS's operation only self-testing will be performed.

**CLASS (A1): VERIFIED DESIGN**

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the **formal** top-level specification. (See the Security Testing Guidelines.) No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. **Manual or other mapping of the FTLS to the source code may form a basis for penetration testing.**

## CLASS (B3): SECURITY DOMAINS

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be **found resistant to** penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification. (See the Security Testing Guidelines.) **No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.**

## CLASS (B2): STRUCTURED PROTECTION

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. **The TCB shall be found relatively resistant to penetration.** All discovered flaws shall be **corrected** and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. **Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification.** (See the Security Testing

Guidelines.)

3.3 Communication Management

3.3.1 Communications Control

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

3.4.A.1 The ERT-TCS will be developed so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

3.4.A.2 The ERT-TCS will be developed so that all multi-level secure unclassified, classified, or otherwise sensitive information transferred into or out of the ERT-TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

Preservation of Integrity

3.4.I.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

Prevention of Compromise

3.4.C.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

Assurance of Service

3.4.S.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

3.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

3.4.S.3 Communications will be available during all operational modes.

3.4.S.4 The ERT-TCS will be developed so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

3.4.S.5 The ERT-TCS will be developed so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

**Operational Environment:**

All Security Mandates

4.4.A.1 The ERT-TCS will be operated so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

4.4.A.2 The ERT-TCS will be operated so that all multi-level secure unclassified, classified, or otherwise information transferred into or out of the ERT-TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

Preservation of Integrity

4.4.I.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

Prevention of Compromise

4.4.C.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

Assurance of Service

4.4.S.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

4.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

4.4.S.3 Communications will be available during all operational modes.

4.4.S.4 The ERT-TCS will be operated so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

4.4.S.5 ERT-TCS will be operated so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

**Maintenance Environment:**

All Security Mandates

5.4.A.1 The ERT-TCS will be maintained so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

5.4.A.2 The ERT-TCS will be maintained so that all multi-level secure unclassified, classified, or otherwise information transferred into or out of the ERT-TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

Preservation of Integrity

5.4.I.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

Prevention of Compromise

5.4.C.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

Assurance of Service

5.4.S.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

5.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

5.4.S.3 Communications will be available during all operational modes.

5.4.S.4 The ERT-TCS will be maintained so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

5.4.S.5 ERT-TCS will be maintained so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

3.3.2 Manual Transfer of Data

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

3.4.A.3 The ERT-TCS will be developed so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

Preservation of Integrity

Prevention of Compromise

3.4.C.2 The ERT-TCS will be developed so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

3.4.C.3 The ERT-TCS will be developed so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing classified and unclassified sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

Assurance of Service

**Operational Environment:**

All Security Mandates

4.4.A.3 The ERT-TCS will be operated so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

Preservation of Integrity

Prevention of Compromise

4.4.C.2 The ERT-TCS will be operated so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

4.4.C.3 The ERT-TCS will be operated so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing unclassified, classified, or otherwise sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.4.A.3 The ERT-TCS will be maintained so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

Preservation of Integrity

Prevention of Compromise

5.4.C.2 The ERT-TCS will be maintained so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

5.4.C.3 The ERT-TCS will be maintained so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing unclassified, classified, or otherwise sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

Assurance of Service

3.3.3 Covert Channel Analysis

These criteria do not apply to the operational environment.

**CLASS (A1): VERIFIED DESIGN**

The system developer shall conduct a thorough search for covert channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.) **Formal methods shall be used in the analysis.**

CLASS (B3): SECURITY DOMAINS

The system developer shall conduct a thorough search for covert channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.) Insert A1's Covert Channel Analysis text.

CLASS (B2): STRUCTURED PROTECTION

**The system developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.)**

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

3.2.C.2 All resources that process unclassified, classified, or otherwise sensitive information will be developed to meet the appropriate radiation limits for the local TEMPEST threat.

3.3.C.5 The ERT-TCS will be designed so that covert channels are prevented or otherwise controlled.

3.3.C.6 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the developmental environment.

3.3.C.7 All products that process unclassified, classified, or otherwise sensitive information will be developed to meet the appropriate radiation limits for the local TEMPEST threat.

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

4.2.C.2 All resources that processes unclassified, classified, or otherwise sensitive information will meet the appropriate radiation limits for the local TEMPEST threat.

4.3.C.4 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the operational environment.

4.3.C.5 All products that processes unclassified, classified, or otherwise sensitive information will meet the appropriate radiation limits for the local TEMPEST threat.

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

5.2.C.2 All resources that process unclassified, classified, or otherwise sensitive information will be maintained to meet the appropriate radiation limits for the local TEMPEST threat.

5.3.C.4 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the maintenance environment.

5.3.C.5 All products that processes unclassified, classified, or otherwise sensitive information will be maintained to meet the appropriate radiation limits for the local TEMPEST threat.

Assurance of Service

## 4 Documentation

### 4.1 Security Features User's Guide

**CLASS (A1): VERIFIED DESIGN**

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

**CLASS (B3): SECURITY DOMAINS**

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

**CLASS (B2): STRUCTURED PROTECTION**

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

### 4.2 Trusted Facility Manual

Only those criteria relevant to the operational environment apply to this environment.

**CLASS (A1): VERIFIED DESIGN**

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for

each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.

CLASS (B3): SECURITY DOMAINS

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. **It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.**

CLASS (B2): STRUCTURED PROTECTION

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and

administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. **The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.**

4.3 Test Documentation

These criteria do not apply to the operational environment.

CLASS (A1): VERIFIED DESIGN

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths. **The results of the mapping between the formal top-level specification and the TCB source code shall be given.**

CLASS (B3): SECURITY DOMAINS

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.

CLASS (B2): STRUCTURED PROTECTION

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security

mechanisms' functional testing. **It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths.**

## 4.4 Design Documentation

These criteria do not apply to the operational environment.

### CLASS (A1): VERIFIED DESIGN

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the **formal top-level specification (FTLS)**. The elements of the FTLS shall be shown, using informal techniques, to correspond to the elements of the TCB. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.) **Hardware, firmware, and software mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O) shall be clearly described.**

## CLASS (B3): SECURITY DOMAINS

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. **The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB.** Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)

## CLASS (B2): STRUCTURED PROTECTION

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. **The** interfaces between **the** TCB modules shall be described. **A formal** description of the security policy model enforced by the TCB shall be available and **proven** that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. **The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel**

**analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.)**

4.5 Documentation Management

**CLASS (A1): VERIFIED DESIGN**

**CLASS (B3): SECURITY DOMAINS**

**CLASS (B2): STRUCTURED PROTECTION**

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

3.3.I.10 Auditing procedures will be established and enforced to track all documentation created and modified during the development of the ERT-TCS. For each document this includes its title, version number, the names of its authors, reviewers, and authorities who approve the document, and its time of creation, revision, circulation, and approval.

Prevention of Compromise

Assurance of Service

3.3.S.6 The product documentation will contain the design of the procedures that will ensure the adequacy of resources to perform, at the very least, the most critical ERT-TCS functions during each operational mode.

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

# SECTION 3.0

# MAPPING OF THE

# TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

# INTO THE

# EMBEDDED REAL-TIME TRUSTED COMPUTER SYSTEM REQUIREMENTS

THIS PAGE IS INTENTIONALLY BLANK.

## 3.1 ORGANIZATION OF THE ERT-TCS RATIONALES

## 3.2 MAPPING OF THE TCSEC INTO THE ERT-TCS REQUIREMENTS (with their rationales)

### I. ALL SECURITY MANDATES

#### 1. ACCREDIT FACILITIES

**Rationale:**

The intent of these requirements is to establish that sufficient security measures have been taken in a facility so that the facility can be trusted to develop, operate, or maintain the ERT-TCS. Satisfying the requirements in this section provides assurance to the designated approving authority that the resources in the accredited facility are approved to operate in a particular security mode using a prescribed set of safeguards.

The accreditation process is based upon a comprehensive security inspection and evaluation of the resources in the facility and the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls. Accreditation confers responsibility to maintain security safeguards upon the official who has the authority to accept the security safeguards prescribed for a facility.

A security policy is the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. It specifies if, when, how, and by whom, and the extent to which the requirements for security are to be addressed. Each facility needs to have a security policy that addresses all the security requirements, and this security policy must be enforced to protect the ERT-TCS in its various environments from threats which could cause compromise, loss of integrity, or denial of service. A facility that does not have an enforced security policy will lack the guidance to preserve security and will be unable to detect a breach of security.

To prevent unnecessary restrictions from being placed on a facility, facilities need only be accredited to perform those activities for which the facility is responsible. Unnecessary restrictions are those restrictions that apply only to activities which the facility will never perform. An activity for which the facility has not been accredited must be prevented. This is to ensure that the appropriate security safeguards are in place and enforced before the activity is allowed to be

performed. For example, a developmental facility which is only responsible for testing the ERT-TCS need only be accredited to perform testing activities, and there must be mechanisms in place and enforced that prevent the performance of activities other than testing.

Accreditation of facilities supports all the security mandates: preserve integrity, prevent compromise, and assure service. A security policy provides rules for supporting all the security mandates. The accreditation process provides assurance that the security policy satisfies the security requirements and that the facility has adequately implemented the security policy. The accreditation process provides a common measure of trust of the facilities (i.e., that the facilities have a common level of trust and items can be transferred between facilities without discrepancies in the care taken for security).

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.1.A.1 Every developmental facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

3.1.1 Facility Accreditation

3.1.A.2 Every developmental facility need only be accredited to perform those activities (e.g., create, modify, enhance, test, or deploy) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

3.1.1 Facility Accreditation

3.1.A.3 Every product will be developed in an accredited facility.

3.1.1 Facility Accreditation

3.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment. For example, while a maintenance facility performs developmental activities (e.g., enhance ERT-TCS software) it will be considered a developmental facility and therefore be accredited in the same manner and to the same degree as any other developmental facility.

3.1.1 Facility Accreditation

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

4.1.A.1 Every operational facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

3.1.1 Facility Accreditation

4.1.A.2 Every operational facility need only be accredited to perform those activities (e.g., power up, operate for a mission, upload or download data, power down from mission) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

3.1.1 Facility Accreditation

4.1.A.3 Every product will be operated in an accredited facility.

3.1.1 Facility Accreditation

4.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment.

3.1.1 Facility Accreditation

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.1.A.1 Every maintenance facility will have a security policy established and enforced that addresses all the security mandates: preserve integrity, prevent compromise, and assure service.

3.1.1 Facility Accreditation

5.1.A.2 Every maintenance facility need only be accredited to perform those activities (e.g., repair hardware, perform preventative maintenance, reconfigure, change security levels, perform self test diagnostics, or storage) that the facility actually performs on resources or products. Also, there must be mechanisms in place and enforced to prevent the performance of activities for which the facility has not been accredited.

3.1.1 Facility Accreditation

5.1.A.3 Every product will be maintained in an accredited facility.

3.1.1 Facility Accreditation

5.1.A.4 While a facility performs activities not associated with the environment in which it resides, the facility will be considered to be in the other environment. That is, the facility will be accredited in the same manner and to the same degree as any other facility in the other environment. For example, while a maintenance facility performs developmental activities (e.g., enhance ERT-TCS software) it will be considered a developmental facility and therefore be accredited in the same manner and to the same degree as any other developmental facility.

3.1.1 Facility Accreditation

Preservation of Integrity

Prevention of Compromise

Assurance of Service

2. CERTIFY RESOURCES AND PRODUCTS

**Rationale:**

The intent of these requirements is to establish a means by which the operations and capabilities of the resources and products within an environment can be trusted (i.e., correct, complete, and provides exact results). Satisfying the requirements in this section provides assurance to the designated approving authority that the resources and products within an environment comply with the security policy.

The certification process is based upon the comprehensive inspection and evaluation of the technical and nontechnical features of the resource or product and other safeguards that establish the extent to which a particular design and implementation meets the security policy. Certification confers security responsibility upon the official who has the authority to approve the implementation of the security policy for the resource or product. The certification process of a resource or product supports the accreditation process and is supported by the creators, maintainers, and reviewers of the resource or product. If the resource or product can not be certified to an adequate level of trust, then the resource or product must be rejected.

Requirements associated with the development environment do not apply to external resources (e.g., commercial off-the-shelf software tools). Instead, they are certified upon entering the ERT-TCS environments. The security policy will define the certification process for external resources. This process must be completed before an external resource can be brought into the environment. Internal resources and products are signed by their creators, maintainers, and reviewers to assign accountability for the compliance with the security policy.

Certification of resources and products supports all the security mandates: preserve integrity, prevent compromise, and assure service. A security policy provides rules for supporting all the security mandates. The certification process provides assurance that the resources and products in a facility comply with the security policy. The certification process provides a common measure of trust of the resources and products within a facility (i.e., that each resource and product with a facility has a common level of trust and each resource can be transferred between facilities without discrepancies in ensuring their security).

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the developmental environment.

3.1.4 Certification

3.2.A.2 Every internal resource will be signed off by the resource's creators, modifiers, and reviewers.

3.1.4 Certification

3.2.A.3 Every internal resource will be certified to comply with the security policy.

3.1.4 Certification

3.2.A.4 Every resource that implements part of the security policy will be certified to be necessary for enforcing the security policy.

3.1.4 Certification

3.2.A.5 Every modified or enhanced internal resource will be subject to the same certification process as the original resource.

3.1.4 Certification

3.3.A.1 Every product will be signed off by the product's creators, modifiers, and reviewers.

3.1.4 Certification

3.3.A.2 Every product will be certified to comply with the security policy.

3.1.4 Certification

3.3.A.3 Every product that implements part of the security policy will be certified to be necessary for enforcing the security policy.

3.1.4 Certification

3.3.A.4 Products will be developed to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

3.2.4 System Integrity

3.3.A.5 Every product will be certified to process the highest classification of information to which it has direct or indirect access.

3.1.4 Certification

3.3.A.6 Every modified or enhanced product will be subject to the same certification process as the original product.

3.1.4 Certification

Preservation of Integrity

3.3.I.1 Every product will be certified to preserve the product's integrity before each time it is deployed.

3.1.4 Certification

Prevention of Compromise

3.3.C.1 Every product will be certified to prevent the product's compromise before each time it is deployed.

3.1.4 Certification

Assurance of Service

3.3.S.1 Every product will be certified to assure the product's service before each time it is deployed.

3.1.4 Certification

**Operational Environment:**

All Security Mandates

4.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the operational environment.

3.1.4 Certification

4.3.A.1 Products will be able to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

3.2.4 System Integrity

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.2.A.1 Every external resource will be certified to comply with the security policy before the resource is allowed to enter or interface with the maintenance environment.

3.1.4 Certification

5.3.A.1 Products will be maintained to allow the ERT-TCS to self test its trusted operations and capabilities for correctness, completeness, and preciseness. These operations will be logged in the audit trail.

3.2.4 System Integrity

Preservation of Integrity

Prevention of Compromise

Assurance of Service

## 3. CONTROL EFFECT OF ERRORS

**Rationale:**

The intent of these requirements is to prevent a failure of security resulting from software, firmware, hardware, or data errors or system failures. Satisfying the requirements in this section provides protection of the ERT-TCS and the data controlled by the ERT-TCS from a breach of security that could be caused by errors which occur during operation of the ERT-TCS.

Mechanisms must exist and be in effect to control the effect of errors or failures so that the ERT-TCS is not vulnerable to security threats. These mechanisms include error prevention mechanisms, error detection mechanisms, error handling mechanisms, audit trails, and fault tolerance techniques. An audit trail enables the reconstruction, reviewing, examination, and analysis of the sequence of events which occurred prior to an error or failure or attempted breach of security to correct the situation and identify the person responsible. Formal reviews of the software, firmware, hardware, and data, as well as functional "walk-throughs" and simulations may be used to establish that sufficient mechanisms have been incorporated into the ERT-TCS to control the effect of errors on security.

The control of errors supports all the security mandates: preserve integrity, prevent compromise, assure service. Because a software, firmware, hardware, data error, or system failure could cause a loss of integrity, compromise, or denial of service, the requirements concerning the control of errors will preserve integrity, prevent compromise, and assure service.

**Security Requirements:**

The following requirements are associated with this rationale.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

3.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

3.2.4 System Integrity

3.3.I.2 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

3.2.4 System Integrity

Prevention of Compromise

3.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.2.4 System Integrity

3.3.C.2 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on compromise will be minimized and be auditable.

3.2.4 System Integrity

Assurance of Service

3.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

3.3.S.2 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

**Operational Environment:**

All Security Mandates

Preservation of Integrity

4.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

3.2.4 System Integrity

4.3.I.1 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on its integrity will be minimized and be auditable.

3.2.4 System Integrity

Prevention of Compromise

4.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.2.4 System Integrity

4.3.C.1 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.2.4 System Integrity

Assurance of Service

4.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

4.3.S.1 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

5.2.I.1 A single resource error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

3.2.4 System Integrity

5.3.I.1 A single product error or failure will not result in the loss of integrity of the ERT-TCS. The effect of subsequent failures on integrity will be minimized and be auditable.

3.2.4 System Integrity

Prevention of Compromise

5.2.C.1 A single resource error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.2.4 System Integrity

5.3.C.1 A single product error or failure will not result in the compromise of the ERT-TCS. The effect of subsequent failures on its compromise will be minimized and be auditable.

3.2.4 System Integrity

Assurance of Service

5.2.S.1 A single resource error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

5.3.S.1 A single product error or failure will not result in the denial of the service of the ERT-TCS to authorized users or subjects. The effect of subsequent failures on denial of service will be minimized and be auditable.

3.2.4 System Integrity

## 4. CONTROL FACILITY ACCESS

**Rationale:**

The intent of these requirements is to prevent unauthorized access to the ERT-TCS facility and to permit authorized access to and within an ERT-TCS facility. Satisfying these requirements in this section provides assurance that access to and within the facility is controlled.

Mechanisms must exist and be in effect to control access to a facility. These mechanisms include configuration management, configuration control, passwords, access lists, control access restrictions, clearance practices, "need-to-know" practices, and audit trails. The "need-to-know" principle minimizes the number of subjects that can access a piece of information. This reduces the risks of erroneous modifications as well as the potential for compromise. Audit trails are used to monitor the access histories of objects by users and subjects. For instance, if an unauthorized attempt is made to access or operate the ERT-TCS, then the attempt must be logged in the audit trail.

The control of facility access supports all the security mandates: preserve integrity, prevent compromise, and assure service. These requirements control the general access to a facility and are the first line of defence to the ERT-TCS and the data controlled by the ERT-TCS.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.1.A.5 Every developmental facility will be secured with controlled access restrictions.

3.1.2 Facility Access Control

3.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

2.2 Audit

3.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

2.2 Audit

3.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

3.1.2 Facility Access Control

3.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, or otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the developmental facility.

3.2.2 Configuration Management

3.2.A.6 Every developmental environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

3.1.2 Facility Access Control

3.3.A.7 Every developmental environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

1.4 Mandatory Access Control

Preservation of Integrity

Prevention of Compromise

3.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the developmental resources and facilities.

3.1.2 Facility Access Control

Assurance of Service

3.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

3.1.2 Facility Access Control

3.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

1.5 Assurance of Authorized Access

**Operational Environment:**

All Security Mandates

4.1.A.5 Every operational facility will be secured with controlled access restrictions.

3.1.2 Facility Access Control

4.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

2.2 Audit

4.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

2.2 Audit

4.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

3.1.2 Facility Access Control

4.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, or otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the operational facility.

3.2.2 Configuration Management

4.2.A.2 Every operational environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

3.1.2 Facility Access Control

4.3.A.2 Every operational environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

1.4 Mandatory Access Control

Preservation of Integrity

Prevention of Compromise

4.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the operational resources and facilities.

3.1.2 Facility Access Control

Assurance of Service

4.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

3.1.2 Facility Access Control

4.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

1.5 Assurance of Authorized Access

4.1.S.3 During a mission, the most critical tasks will always have access to all that they need to function adequately.

1.5 Assurance of Authorized Access

**Maintenance Environment:**

All Security Mandates

5.1.A.5 Every maintenance facility will be secured with controlled access restrictions.

3.1.2 Facility Access Control

5.1.A.6 Actions by authorized personnel or processes will be audited to a level of detail commensurate with the type of access granted to the personnel or process.

2.2 Audit

5.1.A.7 Audit procedures and practices will be defined, implemented, and enforced with respect to each authorized person's or process's performance of duties. For instance, unauthorized requests for access by a subject, including a process, will be logged.

2.2 Audit

5.1.A.8 When the ERT-TCS is operating in a classified mode only authorized personnel or processes (i.e., those personnel or processes with proper clearance and need-to-know) will have access to the ERT-TCS.

3.1.2 Facility Access Control

5.1.A.9 Thorough and stringent configuration management and configuration control of products; resources; unclassified, classified, and otherwise sensitive data; and the media on which they reside will be performed in a trusted manner in the maintenance facility.

3.1.2 Facility Access Control

5.1.A.10 Maintenance may be performed by uncleared personnel only when the ERT-TCS is in an unclassified mode.

3.2.2 Configuration Management

5.2.A.2 Every maintenance environment user or subject attempting access to a resource will be sufficiently authorized, identified, and authenticated before access to the resource is granted.

3.1.2 Facility Access Control

5.3.A.2 Every maintenance environment user or subject attempting to access a product will be sufficiently authorized, identified, and authenticated before access to the product is granted.

1.4 Mandatory Access Control

Preservation of Integrity

Prevention of Compromise

5.1.C.1 The "need-to-know" principle will apply to limit the information flow within or among the maintenance resources and facilities.

3.1.2 Facility Access Control

Assurance of Service

5.1.S.1 Each person who has been cleared to the highest level required for accessing unclassified, classified, or otherwise sensitive information (e.g., documentation, software, firmware, hardware, or data) to which the person requires access to perform his or her functional role will not be denied access to this information.

3.1.2 Facility Access Control

5.1.S.2 The access control mechanisms will permit access by a user or subject to an object that the user or subject is authorized to access.

1.5 Assurance of Authorized Access

## 5. CONTROL COMMUNICATIONS

**Rationale:**

The intent of these requirements is to protect unclassified, classified, and otherwise sensitive data from a security failure during communication. Satisfying the requirements in this section provides protection of the objects that are input into and output from the ERT-TCS from threats that could cause compromise, loss of integrity, or denial of service.

Mechanisms must exist and be in effect to control the ERT-TCS communications so that the ERT-TCS is not vulnerable to security threats. These mechanisms include secured communication channels, insertable and removable storage, erasure mechanisms, encryption mechanisms, and sensitivity labels. Possible covert channels must be identified and controlled to prevent the surreptitious transfer of information. Communication includes memory sharing and message passing handled by the ERT-TCS. Controlled data must be transportable or securable for mode changes.

When unclassified, classified, or otherwise sensitive data is moving either physically or electronically, it is vulnerable to compromise, loss of integrity, or denial of service. Therefore, the requirements that control communications will preserve integrity, prevent compromise, and assure service.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.4.A.1 The ERT-TCS will be developed so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

3.3.1 Communications Control

3.4.A.2 The ERT-TCS will be developed so that all multi-level secure unclassified, classified, or otherwise sensitive information transferred into or out of the ERT-TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

3.3.1 Communications Control

3.4.A.3 The ERT-TCS will be developed so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

3.3.2 Manual Transfer of Data

Preservation of Integrity

3.4.I.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

Prevention of Compromise

3.4.C.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

3.4.C.2 The ERT-TCS will be developed so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

3.3.2 Manual Transfer of Data

3.4.C.3 The ERT-TCS will be developed so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing classified and unclassified sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

3.3.2 Manual Transfer of Data

3.4.C.4 The ERT-TCS will be developed so that all multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

1.3.2 : Exportation and Importation of Labeled Information

Assurance of Service

3.4.S.1 The ERT-TCS will be developed so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

3.3.1 Communications Control

3.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

3.3.1 Communications Control

3.4.S.3 Communications will be available during all operational modes.

3.3.1 Communications Control

**Operational Environment:**

All Security Mandates

4.4.A.1 The ERT-TCS will be operated so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

3.3.1 Communications Control

4.4.A.2 The ERT-TCS will be operated so that all multi-level secure unclassified, classified, or otherwise information transferred into or out of the ERT-TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

3.3.1 Communications Control

4.4.A.3 The ERT-TCS will be operated so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

3.3.2 Manual Transfer of Data

Preservation of Integrity

4.4.I.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

Prevention of Compromise

4.4.C.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

4.4.C.2 The ERT-TCS will be operated so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

3.3.2 Manual Transfer of Data

4.4.C.3 The ERT-TCS will be operated so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing unclassified, classified, or otherwise sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

3.3.2 Manual Transfer of Data

4.4.C.4 All multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

1.3.2 Exportation and Importation of Labeled Information

Assurance of Service

4.4.S.1 The ERT-TCS will be operated so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

3.3.1 Communications Control

4.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

3.3.1 Communications Control

4.4.S.3 Communications will be available during all operational modes.

3.3.1 Communications Control

**Maintenance Environment:**

All Security Mandates

5.4.A.1 The ERT-TCS will be maintained so that all data transmitted between the ERT-TCS and external security controlled systems will be transferred by trusted means over secured communication channels.

3.3.1 Communications Control

5.4.A.2 The ERT-TCS will be maintained so that all multi-level secure unclassified, classified, or otherwise information transferred into or out of the ERT TCS will be transferred and otherwise handled by trusted means commensurate with the level of protection required for the information being transferred.

3.3.1 Communications Control

5.4.A.3 The ERT-TCS will be maintained so that all manual transfer of data to or from the ERT-TCS will be by insertable and removable storage medium.

3.3.2 Manual Transfer of Data

Preservation of Integrity

5.4.I.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the loss of integrity of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

Prevention of Compromise

5.4.C.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the compromise of unclassified, classified, or otherwise sensitive data.

3.3.1 Communications Control

5.4.C.2 The ERT-TCS will be maintained so that when the ERT-TCS changes from operational mode to non-operational mode, all removable data storage media containing unclassified, classified, or otherwise sensitive information will be removed from the ERT-TCS by authorized personnel.

3.3.2 Manual Transfer of Data

5.4.C.3 The ERT-TCS will be maintained so that when the ERT-TCS changes from operational mode to non-operational mode, all non-removable data storage media containing unclassified, classified, or otherwise sensitive information will be erased or encrypted. Erasure will be accomplished in a manner that irrevocably removes all information according to accepted standards for the type of specific media. Encryption will be accomplished using accepted algorithms, implementations, and key management methods.

3.3.2 Manual Transfer of Data

5.4.C.4 The ERT-TCS will be maintained so that all multi-level secure inputs into the ERT-TCS and outputs from the ERT-TCS will be clearly marked (e.g., with sensitivity labels) for identification and authentication by the ERT-TCS and authorized personnel.

1.3.2 Exportation and Importation of Labeled Information

Assurance of Service

5.4.S.1 The ERT-TCS will be maintained so that no communication between ERT-TCBs or between ERT-TCBs and other embedded trusted (sub)system(s) will result in the denial of service to authorized users or subjects.

3.3.1 Communications Control

5.4.S.2 Communication channels between ERT-TCBs will be available to authorized users or subjects during all modes of operation, commensurate with the criticality, priority level, and security of the communication.

3.3.1 Communications Control

5.4.S.3 Communications will be available during all operational modes.

3.3.1 Communications Control

## 6. CONTROL DISTRIBUTION

**Rationale:**

The intent of these requirements is to prevent a failure of security from resulting from the distribution of an object within or between facilities. Satisfying the requirements in this section provides protection of the ERT-TCS and the data controlled by the ERT-TCS from a breach of security that occurs while the objects are being transferred within or among facilities.

Distribution can be by physical means or electronic means. Mechanisms must exist and be in effect to control the distribution of objects so that the ERT-TCS is not vulnerable to security threats. Transfers of resources, products, or data within an environment must not be made from a higher security level object to an object of a lower security level. The restriction of access to information by users, who require the access to, knowledge of, or possession of this information, which is needed to perform official duties, will limit the information flow to necessary information. These controls are to prevent unauthorized access (either read or write) to these items during their distribution. Mechanisms must control the use of repositories of software.

The control of distribution supports all the security mandates: preserve integrity, prevent compromise, and assure service. During the transfer process an object is especially vulnerable to threats to its integrity, compromise, and assurance of service.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.5.A.1 Every product, resource, and unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

3.1.3 Trusted Distribution

Preservation of Integrity

3.5.I.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

3.1.3 Trusted Distribution

Prevention of Compromise

3.5.C.1 The distribution of products, resources, and unclassified, classified, and otherwise sensitive data among resources will not result in their compromise.

3.1.3 Trusted Distribution

3.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

3.1.3 Trusted Distribution

Assurance of Service

3.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

3.1.3 Trusted Distribution

3.5.S.2 No type of distribution will impair the performance of resources.

3.1.3 Trusted Distribution

**Operational Environment:**

All Security Mandates

4.5.A.1 Every product, resource, or unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

3.1.3 Trusted Distribution

Preservation of Integrity

4.5.I.1 The distribution of products, resources, and unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

3.1.3 Trusted Distribution

Prevention of Compromise

4.5.C.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in their compromise.

3.1.3 Trusted Distribution

4.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

3.1.3 Trusted Distribution

Assurance of Service

4.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

3.1.3 Trusted Distribution

4.5.S.2 No type of distribution will impair the performance of resources.

3.1.3 Trusted Distribution

**Maintenance Environment:**

All Security Mandates

5.5.A.1 Every product, resource, or unclassified, classified, or otherwise sensitive data will be transferred or distributed by trusted means appropriate to its level of classification and sensitivity.

3.1.3 Trusted Distribution

Preservation of Integrity

5.5.I.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the loss of their integrity.

3.1.3 Trusted Distribution

Prevention of Compromise

5.5.C.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in their compromise.

3.1.3 Trusted Distribution

5.5.C.2 Contractor, subcontractor, and government classified and unclassified sensitive voice and data communications concerning the ERT-TCS will be by trusted means.

3.1.3 Trusted Distribution

Assurance of Service

5.5.S.1 The distribution of products, resources, or unclassified, classified, or otherwise sensitive data among resources will not result in the denial of service to authorized personnel.

3.1.3 Trusted Distribution

5.5.S.2 No type of distribution will impair the performance of resources.

3.1.3 Trusted Distribution

## II. SECURITY MANDATE TO PRESERVE INTEGRITY

### 7. PREVENT UNAUTHORIZED MODIFICATIONS

**Rationale:**

The intent of these requirements is to prevent unauthorized modifications made to the ERT-TCS's documentation, software, firmware, hardware, or data to provide sufficient assurance that the ERT-TCS is protected against the introduction of unauthorized modifications (e.g., the insertion of malicious logic) that could lead to violations of the security policy. Satisfying the requirements in this section provides protection of the ERT-TCS and the data controlled by the ERT-TCS from modifications made by unauthorized users and subjects.

Mechanisms must exist and be in effect to prevent unauthorized modifications to the ERT-TCS. These mechanisms include access control and configuration management. Access control is the process of limiting access to the resources of a system only to authorized persons, programs, processes, or other systems. The method for enforcing access control includes assigning security levels (which indicate authorization level and sensitivity level) to both subjects and objects. When a subject attempts to write to a specific object, the security level of the subject is compared to that of the object. If the subject's security level is less than or equal to that of the object then access is permitted (i.e., write up is allowed).

The prevention of unauthorized modification includes the enforcement of the write access type (e.g., execute, write, append, modify, delete, or create). Access which has been permitted for one type of access will not result in the access to the ERT-TCS through an unauthorized type of access. Configuration management may assist in restricting types of access.

The prevention of unauthorized modifications supports the "preserve integrity" security mandate. Protection of the ERT-TCS and the data which is controlled by the ERT-TCS from modifications made by unauthorized users or subjects will protect against the loss of integrity.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity :

3.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.3 System Architecture

3.2.I.3 Every resources' software and firmware will be developed to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

3.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

3.2.I.5 The storage media of all resources will be protected from tampering.

3.2.3 System Architecture

3.3.I.3 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.3 System Architecture

3.3.I.4 Every products' software and firmware will be developed to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

3.3.I.5 Every product will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

3.3.I.6 Every transitional ERT-TCS function will be developed to prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

3.2.3 System Architecture

3.3.I.7 The storage media of all products will be protected from tampering.

3.2.3 System Architecture

3.3.I.8 The ERT-TCS will be developed to protect the storage media of all products' software and firmware from tampering.

3.2.3 System Architecture

3.3.I.9 Every product will be developed to process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.2.3 System Architecture

3.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

3.2.3 System Architecture

3.6.I.2 The ERT-TCS will be developed to protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

3.2.3 System Architecture

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

4.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs)

3.2.3 System Architecture

4.2.I.3 Every resources' software and firmware will operate to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

4.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

4.2.I.5 The storage media of all resources will be protected from tampering.

3.2.3 System Architecture

4.3.I.2 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.3 System Architecture

4.3.I.3 Every products' software and firmware will operate to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

4.3.I.4 Every product will be protected from unauthorized modification, [illegible]re, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

4.3.I.5 Every transitional ERT-TCS function will prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

3.2.3 System Architecture

4.3.I.6 The storage media of all products will be protected from tampering.

3.2.3 System Architecture

4.3.I.7 The ERT-TCS will operate to protect the storage media of all products' software and firmware from tampering.

3.2.3 System Architecture

4.3.I.8 Every product will process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.2.3 System Architecture

4.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

3.2.3 System Architecture

4.6.I.2 The ERT-TCS will protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

3.2.3 System Architecture

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

5.2.I.2 No resources' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.3 System Architecture

5.2.I.3 Every resources' software and firmware will be maintained to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

5.2.I.4 Every resource will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

5.2.I.5 The storage media of all resources will be protected from tampering.

3.2.3 System Architecture

5.3.I.2 No products' software or firmware will contain malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.3 System Architecture

5.3.I.3 Every products' software and firmware will be maintained to prevent the introduction of malicious code (e.g., Trojan Horses, viruses, trap doors, time bombs, logic bombs).

3.2.4 System Integrity

5.3.I.4 Every product will be protected from unauthorized modification, erasure, and substitution of its program code, data structures, or information.

3.2.3 System Architecture

5.3.I.5 Every transitional ERT-TCS function will be maintained to prevent the unauthorized permanent loss of any such unclassified, classified, or otherwise sensitive software, firmware, hardware, or data for which the ERT-TCS is responsible during the performance of these functions.

3.2.3 System Architecture

5.3.I.6 The storage media of all products will be protected from tampering.

3.2.3 System Architecture

5.3.I.7 The ERT-TCS will be maintained to protect the storage media of all products' software and firmware from tampering.

3.2.3 System Architecture

5.3.I.8 Every product will be maintained to process and protect from loss of integrity, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.2.3 System Architecture

5.6.I.1 The storage media of all unclassified, classified, and otherwise sensitive data will be protected from tampering.

3.2.3 System Architecture

5.6.I.2 The ERT-TCS will be maintained to protect the storage media of all unclassified, classified, and otherwise sensitive data from tampering.

3.2.3 System Architecture

Prevention of Compromise

Assurance of Service

## 8. PREVENT ERRONEOUS MODIFICATIONS

**Rationale:**

The intent of these requirements is to prevent authorized, but erroneous (accidental or malicious), modifications to the ERT-TCS's documentation, software, firmware, hardware, and data from being made. Satisfying the requirements in this section provides protection of the ERT-TCS from the introduction of erroneous logic or other erroneous modification that could lead to violations of the ERT-TCS's security policy.

Mechanisms must exist and be in effect to prevent erroneous modification. These mechanisms include tracking requirements through the developmental process, accountable mechanisms, configuration management, configuration control, and formal reviews. Configuration management must provide version control for the resources and products in the environment. By restricting modifications to the latest version and granting modification authority to a single user or subject at a time, version control can preserve the integrity of the resource or product. That is, the versions of resources and products are accounted for by configuration management and configuration control. Formal reviews of the software, firmware, hardware, data, and system, as well as functional "walk-throughs" and simulations may be used to prevent the introduction of errors into the ERT-TCS.

These requirements provide assurance that there is consistency between the documentation and the implementation of the ERT-TCS. For each document, version control is accomplished in the configuration management and configuration control process by including the following: the document's title, version number, the names of its authors, reviewers, and authorities who approve the document, and its time of creation, revision, circulation, and approval. This provides an accounting for a different version of each document.

These requirements directly support the "preserve integrity" security mandate. Protection of the ERT-TCS and the data, which is controlled by the ERT-TCS, from erroneous modifications made by authorized users or subjects will protect against the loss of integrity of the ERT-TCS or the data.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.2.A.7 Every internal resource will be developed to satisfy the requirements for correctness, completeness, exactness, and performance integrity and will be subject to rigorous peer review for compliance with the requirements.

3.2.1 Design Specification and Verification

3.3.A.8 Thorough and stringent configuration management and configuration control of all product documents will be enforced to ensure consistency between the documentation and the implementation of the ERT-TCS.

3.2.2 Configuration Management

3.3.A.9 Every product will be developed to satisfy the requirements for correctness, completeness, exactness, and performance integrity and will be subject to rigorous peer review for compliance with the requirements.

3.2.1 Design Specification and Verification

Preservation of Integrity

3.3.I.10 Auditing procedures will be established and enforced to track all documentation created and modified during the development of the ERT-TCS. For each document this includes its title, version number, the names of its authors, reviewers, and authorities who approve the document, and its time of creation, revision, circulation, and approval.

4.5 Documentation Management

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

## 9. RECOVERY FROM UNAUTHORIZED OR ERRONEOUS MODIFICATIONS

**Rationale:**

The intent of these requirements is to provide for the recovery from failures to protect objects from unauthorized or erroneous modifications. Satisfying the requirements in this section allows an ERT-TCS that has been exposed to unauthorized or erroneous modifications to be restored to a state of integrity.

When software, firmware, hardware, and data that has been stored, transmitted, or otherwise exposed to possible unauthorized modifications is detected; this software, firmware, hardware, or data must be identified and authenticated before it is re-introduced into the environment to verify its integrity.

Mechanisms must exist and be in effect to recover from unauthorized or erroneous modification. These mechanisms include audit trails and configuration management. Audit trails enable the reconstruction, reviewing, and examination of the sequence of environments and activities associated with an operation, a procedure, or an event in a transaction from its inception of final results. The tracing of unauthorized or erroneous modifications through an audit trail can be used to reconstruct a modification history of the ERT-TCS so that the unauthorized or erroneous modification can be reversed, rectified, or eliminated. Accountability is used to enable activities on an ERT-TCS to be traced to individuals or subjects who can be held responsible for their actions. Individual accountability is the ability to positively associate the identity of user or subject with the time, method, and degree of access to a system. The recovery process may include eliminating the version of the ERT-TCS that contains the unauthorized modification and reverting to a previous trusted version. Configuration management may be utilized as a recovery mechanism in the development or maintenance environments by restoring a pervious trusted version.

The recovery from the failure to protect objects from unauthorized or erroneous modifications restores the integrity, therefore these requirements support the "preserve integrity" security mandate.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

3.2.I.6 Every internal resource's software and firmware will be developed to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 Trusted Recovery

3.3.I.11 Every product's software and firmware will be developed to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 Trusted Recovery

Prevention of Compromise

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

4.2.I.6 Every internal resource's software and firmware will operate to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 Trusted Recovery

4.3.I.9 Every product's software and firmware will operate with adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 Trusted Recovery

Prevention of Compromise

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

5.2.I.6 Every internal resource's software and firmware will be maintained to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 : Trusted Recovery

5.3.I.9 Every product's software and firmware will be maintained to have adequate recovery procedures to handle malicious or erroneous code when it is discovered.

3.2.5 Trusted Recovery

Prevention of Compromise

Assurance of Service

## III. SECURITY MANDATE TO PREVENT COMPROMISE

### 10. PREVENT UNAUTHORIZED DISCLOSURE

**Rationale:**

The intent of these requirements is to prevent unauthorized disclosure by restricting read access to resources and products to unauthorized individuals, programs, processes, or systems. Satisfying the requirements in this section provide protection to objects from disclosure to unauthorized users or subjects.

Unauthorized read access is prevented through the use of software, firmware, and hardware mechanisms, operating procedures, or management procedures designed to detect and prevent unauthorized access to the environment's resources and products (i.e., access control mechanisms). Access control is the process of limiting access to the resources of a system only to authorized persons programs, processes, or other systems. The method for enforcing access control includes assigning security levels (which indicate authorization level and sensitivity level) to both subjects and objects. When a subject attempts to read from a specific object the security level of the subject is compared to that of the object. If the subjects security level is greater than or equal to that of the object then access is permitted (i.e., read down is allowed). The prevention of unauthorized disclosure includes the enforcement of the read access type (e.g., read or execute). Access that has been permitted for one type of access will not allow an another type of access (which is unauthorized) to the ERT-TCS. For example, if a read access type is authorized but a write access type is unauthorized, then the user (or subject) will be able to read but not to write to an object. Configuration management may assist in restricting types of access.

A user or subject is identified and authenticated as an entity by an ERT-TCS or ERT-TCS development environment. A user or subject is authenticated to verify the identity of a user, device, or other entity in an environment, which is used as a prerequisite to allowing access to resources or products of an environment. Unauthorized access must be prevented by tapping the temporarily inactive terminal of an authorized user. These requirements provide restrictions to prevent a program from accessing data in another user's storage area. The performance of transitional functions can make unclassified, classified, or otherwise sensitive software, firmware, hardware, and data be vulnerable.

Potential covert channels in any ERT-TCS environment need to be detected and prevented, or at least be identified and monitored.

These requirements directly support the "prevent compromise" security mandate. The prevention of unauthorized disclosure supports the "prevent compromise" security mandate. Protection of the ERT-TCS and the data controlled by the ERT-TCS from their disclosures to unauthorized users or subjects will prevent their compromise.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

3.1.A.10 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the developmental facilities. This includes cryptographic information.

3.1.2 Facility Access Control

3.1.A.11 The security level at which the ERT-TCS will be developed will be established and enforced on both the developmental personnel and the environment in which the ERT-TCS is developed.

3.1.2 Facility Access Control

3.2.A.8 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

3.3.A.10 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

3.3.A.11 The ERT-TCS will be developed so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

3.1.2 Facility Access Control

3.3.A.12 The ERT-TCS will be developed so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

3.3.A.13 The ERT-TCS will be developed so that it is capable of powering up and powering down in an unclassified mode. Although the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

3.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

Preservation of Integrity

Prevention of Compromise

3.3.C.3 The ERT-TCS will be developed so that upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

3.1.2 Facility Access Control

3.3.C.4 Every product will be developed to process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

3.3.C.5 The ERT-TCS will be designed so that covert channels are prevented or otherwise controlled.

3.3.3 Covert Channel Analysis

3.3.C.6 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the developmental environment.

3.3.3 Covert Channel Analysis

Assurance of Service

**Operational Environment:**

All Security Mandates

4.1.A.10 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the operational facilities. This includes cryptographic information.

3.1.2 Facility Access Control

4.1.A.11 The security level at which the ERT-TCS operates will be established and enforced on both the operational personnel and the environment in which the ERT-TCS operates.

3.1.2 Facility Access Control

4.2.A.3 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

4.3.A.3 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

4.3.A.4 All products' hardware will be installed and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

4.3.A.5 The ERT-TCS will be operated so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

3.1.2 Facility Access Control

4.3.A.6 The ERT-TCS will operate so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

4.3.A.7 The ERT-TCS will operate so that it is capable of powering up and powering

down in an unclassified mode. Though the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

4.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

Preservation of Integrity

Prevention of Compromise

4.3.C.2 Upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

3.1.2 Facility Access Control

4.3.C.3 Every product will process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

4.3.C.4 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the operational environment.

3.3.3 Covert Channel Analysis

Assurance of Service

**Maintenance Environment:**

All Security Mandates

5.1.A.11 Storage facilities will be established as control areas capable of providing protection for all open storage of information at the classification and sensitivity level of the information used within the maintenance facilities. This includes cryptographic information.

3.1.2 Facility Access Control

5.1.A.12 The security level at which maintenance will be performed on the ERT-TCS will be established and enforced on both the maintenance personnel and the environment in which the maintenance is to be performed.

3.1.2 Facility Access Control

5.2.A.3 Every resource will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

5.3.A.3 Every product will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

5.3.A.4 The ERT-TCS will be maintained so that only an authorized user or subject or trusted software and firmware will initiate and control the transitional functions (e.g., power up, reconfiguration, security level changes, or shutdown) of an ERT-TCS.

3.1.2 Facility Access Control

5.3.A.5 The ERT-TCS will be maintained so that it always controls access to all unclassified, classified, and otherwise sensitive information handled by the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

5.3.A.6 The ERT-TCS will be maintained so that it is capable of powering up and powering down in an unclassified mode. Though the ERT-TCS may be operating in unclassified mode, it will still protect all unclassified, classified, and otherwise sensitive products' software, firmware, hardware, and data in the system in which the ERT-TCS is embedded.

3.1.2 Facility Access Control

5.6.A.1 All data will be stored and protected at a level commensurate with its level of classification and sensitivity.

3.1.2 Facility Access Control

Preservation of Integrity

Prevention of Compromise

5.3.C.2 The ERT-TCS will be maintained so that upon normal and emergency shutdown, all unclassified, classified, and otherwise sensitive data will be purged according to the accepted standard for the type of storage media.

3.1.2 Facility Access Control

5.3.C.3 Every product will be maintained to process and protect from compromise, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

5.3.C.4 Covert channels will be controlled to prevent the compromise of unclassified, classified, or otherwise sensitive information handled in the maintenance environment.

3.3.3 Covert Channel Analysis

Assurance of Service

## 11. CONTROL EMANATIONS

**Rationale:**

The intent of these requirements is to prevent unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose unclassified, classified, or otherwise sensitive information. Satisfying the requirements in this section provides protection of objects from disclosure to unauthorized users or subjects as a result of emanations from ERT-TCS facilities. The intent is to deny unauthorized persons information of value that might be derived from the interception and analysis of compromising emanations from ERT-TCS facilities. For example, emanations from any ERT-TCS environment that could become possible covert channels need to be detected or at least be identified and monitored, so that security is not compromised. The potential compromise of security posed by overt channel emanations must be prevented or at least monitored.

These requirements directly support the "prevent compromise" security mandate.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

3.2.C.2 All resources that process unclassified, classified, or otherwise sensitive information will be developed to meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

3.3.C.7 All products that process unclassified, classified, or otherwise sensitive information will be developed to meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

Assurance of Service

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

4.2.C.2 All resources that processes unclassified, classified, or otherwise sensitive information will meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

4.3.C.5 All products that processes unclassified, classified, or otherwise sensitive information will meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

Assurance of Service

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

5.2.C.2 All resources that process unclassified, classified, or otherwise sensitive information will be maintained to meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

5.3.C.5 All products that processes unclassified, classified, or otherwise sensitive information will be maintained to meet the appropriate radiation limits for the local TEMPEST threat.

3.3.3 Covert Channel Analysis

Assurance of Service

## IV. SECURITY MANDATE TO ASSURE SERVICE

### 12. ASSURE AUTHORIZED ACCESS

**Rationale:**

The intent of these requirements is to ensure necessary access to the resources and products of an environment to authorized, personnel, programs, processes, and other systems. Satisfying the requirements in this section provides assurance that access to objects by authorized users or subjects is not denied.

All resources and products of an environment must be available to an authorized user for the authorized access type (e.g., read, execute, write, append, modify, delete, or create) in an authorized form, at an authorized time. Denial of service of these resources and products must be prevented. Denial of service is any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes delay of service.

Access is permitted through the use of software, firmware, and hardware features, operating procedures, management procedures, and their various combinations designed to detect and permit authorized access to the resources and products of an environment (e.g., ERT-TCS or product documentation). Configuration management systems grant an authorized subject access to the appropriate version of the object.

Assuring authorized access supports the "assure service" security mandate. If authorized users or subjects are denied the service of a resource or product then the ERT-TCS can not be developed, operated, or maintained as required.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.2.S.2 Every internal resource will be developed to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

3.3.S.3 Every product will be developed to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

3.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

3.1.2 Facility Access Control

3.6.S.1 Authorized development personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

3.1.2 Facility Access Control

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

4.2.S.2 Every internal resource will process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

4.3.S.2 Every product will process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

4.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

3.1.2 Facility Access Control

4.6.S.1 Authorized operational personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

3.1.2 Facility Access Control

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

5.2.S.2 Every internal resource will be maintained to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

5.3.S.2 Every product will be maintained to process and protect from denial of service, multi-level secure information in a trusted environment, including the ERT-TCS's runtime environment.

3.1.2 Facility Access Control

5.5.S.3 Every authorized user or subject will have access to all resource distribution mechanisms so that each can have access to all resources that are only available through these mechanisms. This assurance of the service to the distribution mechanisms will be specified in the security policy.

3.1.2 Facility Access Control

5.6.S.1 Authorized maintenance personnel will have access to only that data to which each requires access and to which each has been granted by the security administrator. This access will be on a "need-to-know" basis according to the Least Privilege Principle.

3.1.2 Facility Access Control

13. PROVIDE SUFFICIENT SERVICES

**Rationale:**

The intent of these requirements is to provide confidence that there will be no condition in which insufficient services are available to perform the security functions as specified by the system design and use. Satisfying the requirements in this section provides assurance that there are sufficient services available to perform security function.

The issues that need to be addressed are the allocation of resources, as well as utilization of shared resources, redundant resources, and backup resources.

If an ERT-TCS services are inadequate for its proper operation, then the security, safety, or successful execution of a mission may be threatened. Therefore, these requirements support the "assure service" security mandate.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.3.S.4 All ERT-TCS's modes of operation and ERT-TCS transitional functions will be developed to ensure adequate products' software and firmware and hardware to perform, at least, the most critical ERT-TCS functions.

3.2.3 System Architecture

3.3.S.5 All products will be able to satisfy their performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

3.2.3 System Architecture

3.3.S.6 The product documentation will contain the design of the procedures that will ensure the adequacy of resources to perform, at the very least, the most critical ERT-TCS functions during each operational mode.

4.5 Documentation Management

3.4.S.4 The ERT-TCS will be developed so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

3.3.1 Communications Control

3.4.S.5 The ERT-TCS will be developed so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

3.3.1 Communications Control

3.4.S.6 The ERT-TCS will be developed so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

3.2.3 System Architecture

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

4.3.S.3 All ERT-TCS's modes of operation and ERT-TCS transitional functions will be operated to ensure adequate products' software and firmware and hardware to perform, at least, the most critical ERT-TCS functions.

3.2.3 System Architecture

4.3.S.4 All products will satisfy its performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

3.2.3 System Architecture

4.4.S.4 The ERT-TCS will be operated so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

3.3.1 Communications Control

4.4.S.5 The ERT-TCS will be operated so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

3.3.1 Communications Control

4.4.S.6 The ERT-TCS will be operated so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

3.2.3 System Architecture

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

5.3.S.3 All ERT-TCS's modes of operation and ERT-TCS transitional functions will be maintained to ensure adequate products' software and firmware and hardware to perform, at least, the most critical ERT-TCS functions.

3.2.3 System Architecture

5.3.S.4 All products will be able to satisfy its performance requirements while also satisfying the ERT-TCS's security mandates with the additional execution and memory demands imposed by the incorporation of trusted software and trusted firmware.

3.2.3 System Architecture

5.4.S.4 The ERT-TCS will be maintained so that no communications between ERT-TCBs, or between ERT-TCBs and (sub)systems external to the ERT-TCS, will unduly hinder the performance of the avionics system or the airframe.

3.3.1 Communications Control

5.4.S.5 The ERT-TCS will be maintained so that no communications will consume that which is necessary for more critical or higher priority ERT-TCS functions.

3.3.1 Communications Control

5.4.S.6 The ERT-TCS will be maintained so that no ERT-TCS function will unduly hinder the performance of the avionics system or the airframe.

### 3.2.3 System Architecture

## 14. CONTROL PERFORMANCE DEGRADATIONS

**Rationale:**

The intent of these requirements is to prevent performance degradation of the security features of the critical functions of the ERT-TCS. Satisfying the requirements in this section are associated with the recovery from the loss of services.

Performance degradation implies the prioritization of system functions and a scheme for controlling failures. Considerations in the requirement specifications, design, and implementation must be made to accommodate the presents of the ERT-TCS. Such considerations include dynamic memory, storage, bus bandwidth, processor speed, timing, scheduling, and memory management. If a system can not have its performance degraded gracefully, then the security, safety, or successful execution of a mission may be threatened. Items which must be monitored and controlled are runaway processes, hogging processor time, and starving processing. Useful activities to be managed include controlling, killing, and postponing an individual process.

The loss of an ERT-TCS's resource(s) can threaten the viability of the ERT-TCS during a mission. Therefore, the requirements associated with controlled performance reduction support the "assure service" security mandate.

**Security Requirements:**

The following requirements are associated with this rationale.

**Developmental Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

3.3.S.7 Every product will be developed to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

3.2.3 System Architecture

**Operational Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

4.3.S.5 Every product will operate to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

3.2.3 System Architecture

**Maintenance Environment:**

All Security Mandates

Preservation of Integrity

Prevention of Compromise

Assurance of Service

5.3.S.5 Every product will be maintained to allow its performance not to be unduly degraded by a failure to or reduced performance of any of its subsystems (in particular its ERT-TCBs). That is, every ERT-TCS will be fault tolerant, e.g., by the use of redundant subsystems, such as its ERT-TCBs.

3.2.3 System Architecture